ASSET MANAGEMENT STANDARD

Introduction

Purpose

The purpose of this document is to guide project and operation teams in the expectations of the Cyber Risk and Resilience team regarding asset management for physical, virtual, and informational assets. It outlines the Cybersecurity team's requirements and recommendations in order to ensure cybersecurity risks are mitigated to the university's acceptable level.

This standard is developed as part of the Monash University (MU) cybersecurity standards. This standard will point to baselines to explain specifically where required. Please refer to the cybersecurity standards for specific security requirements (e.g., approved encryption algorithms).

Please engage the Cybersecurity Architecture team for any clarification and if certain service categories or design considerations are not covered by this standard.

In Scope

In the scope of this document:

- Information and data assets
- System, platform and end-users assets
- Asset documentation such as low level and as-built design documents

Out of Scope

Out of the scope of this document:

- Relevant management and operation models
- Security training and awareness requirements
- Step by step implementation guides

RACI Matrix

Actions	Cyber Security	Application Owners	Infrastructure Teams
Develop and maintain security standards	R/A	I/C	I/C
Develop applications in line with security standards	C/I	R/A	C
Implement and maintain infrastructure security in line with security standards	C/I	R/A	R/A

Attributes

Attributes Supported: Protected, Secure, Trusted, Auditable, Isolated, Identified, Resilient, Zoned

Security Architecture Principles

Cyber Security Architecture Principles should be considered in order to protect Monash University's environment.

Security Standard for Asset Management

This section covers the minimum security controls for an asset management plan.

Table 1. Minimum Security Requirements		
NIST CSF Function	**Controls**	**Requirements**
Identify	Governance, Risk and Compliance	• Reference risk management policy and procedures are in place and being complied with. Upon a related change, system owners should consult this standard and its related baselines. Should the use cases not be covered, they should commence a risk assessment as per the MU risk management system. • Applicable legal and regulatory requirements are formally identified based on the information classification. Environment ownership and responsibilities should be identified, including a RACI matrix. • Should an internal or external audit be required, system owners should maintain the required audit artefacts, including but not limited to configuration snapshots, logs and process documents. • Compliance with the Acceptable use policy should be maintained. • Information classification policy and procedures should be in place, and should be complied with.

	Asset Management	• Compliance with MU asset management policy should be maintained.
		• An inventory of systems and software used should be recorded, regularly reviewed, and maintained.
		• The following details are required, at a minimum:
		  ○ IP address(es).
		  ○ Hostname.
		  ○ Location.
		  ○ Software installed.

		○ Purpose of server. ○ Integrations. ○ Person responsible. ○ Team responsible. ○ Information classification level of the system. ● Links to the most recent documentation i.e. as-built, should be provided as part of the MU Configuration Management Database.
	Identity and Access Management	● While managing information assets, MU standard Identity and access management policies and procedures should be complied with.
	Information Asset Lifecycle management	● Information assets should be classified and handled in line with the Information Classification Standard. ● The Service Governance Team's procedures should be in place, and should be followed, to onboard new information assets. ● Cyber security controls, such as encryption, data integrity management, and endpoint security should be in place in line with the Minimum Cybersecurity Standards, to protect information in use, at rest, and in transit. ● Appropriate Data Lifecycle Management (DLM) practices should be followed, this includes but not limited to, backup, archiving, retention and disposal of information assets in accordance with the Information Classification Standard, and inline with any regulatory requirements . ● Refer to the User Device Services (Asset Management) team for specific procedures and processes around disposal of assets. ● The effectiveness of the DLM should be tested and verified regularly.
	Information Asset Management: Policy and Procedures	● System Lifecycle Management (SLM) processes, such as commissioning and decommissioning of systems, software, and platforms should be governed in accordance with the Service Governance Team's onboarding processing documentation.

		• An inventory of the system and platform devices should be maintained as a single point of truth within the MU Configuration Management Database. • MU approved automated asset discovery tools should be used to detect new systems and assets. • Systems and platforms should be security hardened and the hardening status should be continually monitored in accordance with industry best practice and the MU Minimum Cybersecurity standards and checklists.
	Information Asset Management: End-user Device Management	• An inventory of the end-users devices should be maintained as a single point of truth within the MU Configuration Management Database. • Personnel (staff, contractors, etc) in possession of MU computing devices should return these assets in accordance with the Acceptable use policy.
	Information Asset Management: Handling of Removable Media Devices	• Sensitive content stored or transferred on removable media should be encrypted in line with MU cryptography guidelines, and removed if no longer needed. • Any media being transferred by a third party should be logged, and the third party should be an enterprise approved service provider.
Protect	Identity and Access Management	• Access to information assets should be controlled in line with the Identity and Access Management Standard.

Reference

- Monash University Cyber Security Architecture Principles
- Monash University cybersecurity standards
- Monash University Vulnerability Management Baseline

Definitions

Table 2: Definitions	
Term	**Definition**
MU	Monash University.
Information owner	The owner of any form of intellectual property.
Information custodian	Person(s) responsible for the operation and management of systems which collect, manage and/or distribute data.
Information asset	A collection of data that has inherent or recognised value to an organisation.

Version and Update History

Version	Date	Author	Summary of Change
0.1 Draft	18/11/2021	Ashley Niklaus	Initial Draft
0.9 Draft	3/12/2021	Cyber Arch	Peer Review
1.0	9/12/2021	Dan Maslin	Initial Release
1.1	5/06/2024	Ashok Khatiwada	Minor update to wordings